CLAIMS:

1. A method of authorizing an operation requested by a first user on a content item in accordance with a user right identifying a second user and authorizing the second user to perform the requested operation on the content item, in which the operation is authorized upon receipt of information linking a user right of the first user and the user right of the second user.

2. The method of claim 1, in which the information comprises one or more domain certificates identifying the first and second users as members of the same authorized domain.

3. The method of claim 2, in which the one or more domain certificates comprise a first domain certificate identifying the first user as a member of an authorized domain, and a second domain certificate identifying the second user as a member of the authorized domain.

4. The method of claim 2, in which the one or more domain certificates comprise a single certificate identifying the first and second users as members of the authorized domain.

5. The method of claim 1, in which the operation comprises at least one of: a rendering of the content item, a recording of the content item, a transfer of the content item and a creation of a copy of the content item.

6. The method of claim 1 or 2, comprising receiving a content right containing necessary information for performing the requested operation on the content item, the user right of the second user authorizing the second user to employ the content right.

7. The method of claim 6 as dependent from claim 2, in which the operation is not authorized if the content right does not identify the authorized domain.

8. A device arranged to perform an operation requested by a first user on a content item in accordance with a user right identifying a second user and authorizing the second user to perform the requested operation on the content item, being arranged to authorize the operation upon receipt of of information linking a user right of the first user and the user right of the second user.

9. The device of claim 8, in which the information comprises one or more domain certificates identifying the first and second users as members of the same authorized domain.

10. The device of claim 9, in which the one or more domain certificates comprise a first domain certificate identifying the first user as a member of an authorized domain, and a second domain certificate identifying the second user as a member of the authorized domain.

11. The device of claim 9, in which the one or more domain certificates comprise a single certificate identifying the first and second users as members of the authorized domain.

12. The device of claim 8, being arranged to receive an identifier for the first user from an identification device and to perform the operation if the received identifier matches the identification of the first user in the user right of the first user.

13. The device of claim 8 or 9, being arranged to receive a content right containing necessary information for performing the requested operation on the content item, the user right of the second user authorizing the second user to employ the content right.

14. The device of claim 11, in which at least a portion of the content right is encrypted using an encryption key for which a corresponding decryption key is available to the device.

15. The device of claim 13, in which the content right is provided with a digital signature allowing verification of the authenticity of the content right.

16. The device of claim 15, being arranged to perform the operation if the digital signature can be verified successfully using a digital certificate associated with an authorized content provider.

17. The device of claim 15, being arranged to perform the operation if the digital signature can be verified successfully using a digital certificate associated with a particular device.

18. The device of claim 15, being arranged to refuse to perform the operation if the digital signature cannot be verified successfully using a digital certificate associated with an authorized content provider and a digital watermark associated with the authorized content provider is present in the content item.

19. The device of claim 13 or 15, being arranged to extract a public key from the content right and to use the extracted public key in determining whether the operation is authorized.

20. The device of claim 13, being arranged to determine a robust fingerprint for the content item and to refuse to perform the operation if the determined robust fingerprint does not match a robust fingerprint comprised in the content right.

21. The device of claim 13 as dependent from claim 9, being arranged to refuse to perform the operation if the authorized domain is not identified by the content right.

22. A method of authorizing an operation requested by a first user on a content item in accordance with a content right containing necessary information for performing the requested operation on the content item and a user right identifying the first user and authorizing the first user to employ the content right.

23. A device arranged to perform an operation requested by a first user on a content item in accordance with a content right containing necessary information for performing the requested operation on the content item and a user right identifying the first user and authorizing the first user to employ the content right.

24. The device of claim 23, in which at least a portion of the content right is encrypted using an encryption key for which a corresponding decryption key is available to the device.

25. The device of claim 23, in which the content right is provided with a digital signature allowing verification of the authenticity of the content right.

26. The device of claim 25, being arranged to perform the operation if the digital signature can be verified successfully using a digital certificate associated with an authorized content provider.

27. The device of claim 25, being arranged to perform the operation if the digital signature can be verified successfully using a digital certificate associated with a particular device.

28. The device of claim 25, being arranged to refuse to perform the operation if the digital signature cannot be verified successfully using a digital certificate associated with an authorized content provider and a digital watermark associated with the authorized content provider is present in the content item.

29. The device of claim 23, being arranged to determine a robust fingerprint for the content item and to refuse to perform the operation if the determined robust fingerprint does not match a robust fingerprint comprised in the content right.

30. The device of claim 23, being arranged to receive an identifier for the first user from an identification device and to perform the operation if the received identifier matches the identification of the first user in the user right.